Statement

of Andrew Howell

Vice President of Homeland Security Policy

U.S. Chamber of Commerce

ON: **"Helping Business Protect the Homeland: Is the Department of Homeland Security Effectively Implementing the Safety Act?"**

TO: **The House of Representatives Committee on Homeland Security Subcommittee on Emergency Preparedness, Science and Technology and the Subcommittee on Management, Integration and Oversight**

DATE: **September 13, 2006**

The Chamber's mission is to advance human progress through an economic, political and social system based on individual freedom, incentive, initiative, opportunity and responsibility.

Andrew Howell, Vice President of Homeland Security Policy
U.S. Chamber of Commerce

"Helping Business Protect the Homeland: Is the Department of Homeland Security Effectively Implementing the SAFETY Act?"

Before the House of Representatives Committee on Homeland Security
Subcommittee on Emergency Preparedness, Science and Technology and
The Subcommittee on Management, Integration and Oversight

September 13, 2006

Introduction

I would like to thank Chairman Rogers, Chairman Reichert, Representative Meek and Representative Pascrell, and all Members of the Subcommittee on Management, Integration and Oversight, as well as the Subcommittee on Emergency Preparedness, Science and Technology, for giving me the opportunity to testify before you today.

My name is Andrew Howell, and I am the Vice President for Homeland Security Policy at the U.S. Chamber of Commerce. The U.S. Chamber of Commerce ("the Chamber") is the world's largest business federation, representing more than 3 million businesses through our federation, which includes direct corporate members of all types and sizes; trade and professional associations; state and local chambers through the United States; and 104 American Chambers of Commerce abroad (AmChams) in 91 countries.

On behalf of the Chamber, I would like to express our appreciation to the two subcommittees for providing this opportunity to comment on the implementation of the "Support Anti-Terrorism by Fostering Effective Technologies Act (SAFETY Act)". We applaud your efforts to bring attention to this important program, which is one of the few incentives offered to spur the development and deployment of cutting-edge technologies, services and systems to protect our homeland. The Chamber believes that ensuring the security of our citizens should be America's top priority. The SAFETY Act is an important tool necessary to realize that objective, and one that helps to harness the creativity and innovation of the private sector. We look forward to working with members of this committee, and the appropriate subcommittees, as you conduct important oversight of this key DHS program.

The Final SAFETY Act Implementing Regulation

The Chamber applauds the Department of Homeland Security in its efforts to ensure that the SAFETY Act provides the full protections intended by Congress. The final regulations issued on June 8, 2006 provide much-needed certainty on this critical program in several key areas:

- The definition of an act of terrorism;
- Coordination of the timing of SAFETY Act awards with important federal anti-terrorism procurements;

- Explanation of the relationship between the SAFETY Act and indemnification under Public Law 85-804; and
- A concrete process for the use of SAFETY Act protections *en masse* through "block designations and "block certifications."

Additionally, we were pleased to see an explicit process for SAFETY Act awards when products are in the developmental test and evaluation phase, which can either test a promising anti-terrorism technology or identify something that may form the basis for future anti-terrorism technologies.

Let me now expand on each of these areas, which we consider to be among the most important parts of the new regulation.

Definition of an act of terrorism

As you know, terrorism is a global issue that demands a global policy response. For example, Homeland Security Presidential Decision Directive 13 notes that:

> *The security of the Maritime Domain is a global issue. The United States, in cooperation with our allies and friends around the world and our state, local and private sector partners, will work to ensure that lawful private and public activities in the Maritime Domain are protected against attack and criminal and otherwise unlawful or hostile exploitation.*

Additionally, the Container Security Initiative, announced several years ago by former Customs and Border Protection Commissioner Robert Bonner, is based on the principal of "pushing our border out" by stationing U.S. Customs and Border Protection officers at foreign ports shipping goods to the United States.

However, as we all know, U.S. regulation does not easily reach foreign shores. Given this reality, in the context of the SAFETY Act and the global nature of our homeland security policy, how can the government effectively protect firms providing anti-terrorism technologies abroad, where U.S. regulations have limited impact?

Recognizing the need to think differently on the liability threat facing firms selling anti-terrorism technologies that would carry out U.S. policy objectives, our comments in August of 2003 on the proposed SAFETY Act regulation, pointed out the need to clarify the definition of an "Act of Terrorism" to provide clarity for vendors selling anti-terrorism technologies for deployment abroad.

In the final SAFETY Act implementing regulation, DHS offers thoughtful language in this regard, noting that "The Department does not interpret the language of the [SAFETY] Act to impose a geographical restriction for purposes of determining whether an act may be deemed an 'Act of Terrorism' ". Additionally, the regulation notes that "an act on foreign soil may indeed be deemed an 'Act of Terrorism' for purposes of the SAFETY Act provided that it causes harm

in the United States. The Department interprets 'harm' in this context to include harm to financial interests."

In our view, this appropriately protects vendors with financial interests—including equity stakes, shareholders, plants, assets and the like—from an Act of Terrorism abroad if it affects the value of those financial interests in the United States.

Relationship between the SAFETY Act and indemnification under Public Law 85-804

At the same time, there may be areas where this definition does not sufficiently protect a firm with an overseas deployment of technology—particularly if a product liability lawsuit is brought in a court outside of the United States.

Therefore, we believe it is necessary, in some cases, to combine SAFETY Act protections with the benefits of Public Law 85-804, which allows the Government to indemnify private parties acting on the Government's behalf. In our view, those deploying anti-terrorism technology abroad in support of U.S policy to push our borders out, are, in effect, acting on the government's behalf. Therefore, these technologies would be obvious candidates for a dual track SAFETY Act/P.L. 85-804 approach.

This is something we have been calling for since our comments of August 2003 on the Proposed Implementing Regulations for the SAFETY Act. We are pleased that the department, in this final regulation, acknowledges that a combined SAFETY Act/P.L. 85-804 approach "might appropriately be made available." At the same time, we look forward to seeing further guidance from DHS in this area so that important programs with both domestic and international deployments—like perhaps SBINet—can benefit from a strong pool of bidders, undeterred by potential liability concerns.

Coordination with anti-terrorism procurements

Regardless of the location of the anti-terrorism technology deployment, however, one very basic element of a comprehensive SAFETY Act program implementation has been lacking—coordination between acquisition and procurement and SAFETY Act determinations.

The Chamber, in collaboration with our members and several other trade associations, has been working hard with procurement officials and DHS leadership to build SAFETY Act provisions into important procurements. However, this approach has been haphazard and has too often been in reaction to a procurement that has already been issued.

Recently, as well as in this final SAFETY Act rule, DHS has appropriately recognized the need to coordinate SAFETY Act benefit determinations with acquisition and procurement operating procedures. The establishment of a "Pre-Qualification Designation Notice," is a good tool for federal buyers to use during the early stages of acquisition and would be accompanied by an "expedited review of a streamlined application for SAFETY Act coverage…and, in most instances, establish the presumption that the technology under consideration constitutes a QATT" (i.e. qualified anti-terrorism technology), according to the new regulation.

We are also pleased to see this rule states that the Office of SAFETY Act Implementation (OSAI) may also expedite applications for vendors responding to an ongoing solicitation and that the Department may unilaterally decide that a procurement is eligible under the SAFETY Act. While there are still details to be worked out—for example, the timeline for an application being expedited—these are all steps in the right direction.

However, all the process improvements in the world will not help unless DHS simultaneously strengthens its procurement and acquisition corps. We need to find a way to help DHS procurement officials better research markets; plan their procurements; develop meaningful performance metrics; and buy goods and services cost effectively. Incorporating the SAFETY Act into the process of planning an acquisition is essential, and because it is a new program, training will be absolutely essential. By taking the time to carefully consider performance metrics, liability concerns and the role of the SAFETY Act prior to developing and issuing a request for proposals (RFP), our government, our citizenry and the anti-terrorism technology vendor community can do a better job managing risk and protecting our homeland.

Block designations and block certifications

Another area where DHS has made significant progress in this final regulation is the strong statement made for block designations and block certifications. The department decides that all solutions or products that meet a certain specification can be deemed to have streamlined SAFETY Act reviews.

From our perspective, there are several programs where this mechanism should be used in the near term. One that comes to mind is the Registered Traveler (RT) program. Vendors of RT solutions, as you may know, will all have to meet a certain specification set by the Transportation Security Administration. Therefore, it would make sense to designate or certify this group of services, which will be more widely deployed later this year.

At the same time, it is worth noting that the block designations section of the new SAFETY Act kit is the only place in the entire document that makes mention of a "streamlined" process. We believe that there are many areas where DHS can and should streamline the technology evaluation process, and we are eager to understand how the Department intends to carry this out.

Developmental test and evaluation efforts

One final area in the final regulation that merits attention is the section on developmental testing and evaluation designations. The SAFETY Act is designed to spur the development of new technologies; this specific category of SAFETY Act application provides further details on exactly how DHS plans to work with industry partners to protect them from liability in the risky, early stages of a program. We all know that liability can, indeed, extend all the way back to the development phases of a technology. Therefore, awarding SAFETY Act benefits is entirely appropriate.

Of course, once the benefits of the developmental test and evaluation segment of a SAFETY Act certification's benefits have expired—presumed to be 36 months in the regulation and kit—some applicants will, we hope, want to extend their coverage. How DHS handles the continuation of benefits—whether a firm has to fill out an entirely new kit, simply file a modification application, or exercise some other alternative—will need to be worked out. We are eager to see exactly how that process will work, and we will work with DHS to ensure that it functions smoothly and effectively for both the government and the applicant.

Beyond the Implementing Regulations—Making the SAFETY Act Reach its Potential as an Anti-Terrorism Tool

In order to make the SAFETY Act reach its true potential, DHS must implement several new and updated business processes.

The first such process is a new application kit. Now open for public comment, we believe this new kit effectively asks applicants for the information the Department is now actually using to make evaluation decisions. At the same time, while the questions asked are more precise and better guide applicants to provide the right data, we believe the overall burden on the applicants does not, at this point, seem to be reduced.

Therefore, we hope that DHS will continue to work with us and others to limit the amount of information that application evaluators seek, while also making the SAFETY Act process as effective as possible.

We also hope that DHS will soon develop and publish a streamlined SAFETY Act kit. In September, the Chamber joined with a host of other organizations—including the Professional Services Council, the National Defense Industrial Association; the Information Technology Association of America and the Aerospace Industries Association—to develop our version of an effective, streamlined kit for use in specific circumstances. Attached for the record is a letter transmitting our vision of an effective streamlined kit, complete with instructions for DHS.

In this document, we focused on gaining efficiencies and reducing redundancies across the Department. In our view, there is significant overlap between the SAFETY Act office's evaluation process and the review a procurement officer leads when assessing the efficacy of a product, service or integrated solution. As a result, we believe that for purposes of the SAFETY Act, deference can and should be given to the procurement evaluation—whether for an ongoing solicitation or for a prior procurement.

Of course, with regard to procurement, we must congratulate DHS officials for the many strides they have made to more effectively link SAFETY Act determinations and procurement awards. DHS thoughtfully issued a revised Request for Proposal (RFP) for its Advanced Spectroscopic Portal monitor procurement that included SAFETY Act protection for the winning bidder after realizing the liability challenges vendors would face from deploying this bleeding-edge technology. On its SBINet procurement, DHS included language in the original document, and then supplemented it with subsequent modifications.

However, in both of these cases, the SAFETY Act was omitted in the initial procurement process, leaving thoughtful DHS officials to address the liability issue once bidders began asking how their liability concerns would be addressed. As we all know, issuing a procurement is the end of a process which begins with market research and continues through the establishment of program requirements and metrics. To date, federal government acquisition professionals have not systematically included consideration of liability issues—and utilization of the SAFETY Act to mitigate those issues—early in the overall acquisition process. As a result, those of us working on this program from the outside are left at the very last moment—preparation of a request for proposals—to try and have the SAFETY Act integrated into the procurement.

In order to achieve this, changes must be made to both the Department's acquisition regulations as well as the Federal Acquisition Regulation (FAR). We understand both are underway, and that is to be applauded. As soon as the Department and the FAR Council (which recommends changes to the federal purchasing rules) finish their work, the SAFETY Act can systematically be integrated into anti-terrorism procurements across the government

Once these steps have been taken, of course we anticipate there would be aggressive training of acquisition and procurement staff across the government. DHS and other federal acquisition and procurement officials need to better understand the SAFETY Act and appreciate how it provides benefits to buyers and vendors.

At the same time, guidance for state and local buyers—especially those receiving federal money to buy anti-terrorism equipment, services, technology and the like—is essential. Because federal tax dollars are being spent to secure our homeland at the local level, and because the SAFETY Act is not just for federal anti-terrorism procurements, DHS officials should find ways to educate the state and local homeland security community. By taking this step, state and local officials could either incorporate the Act into their acquisition process or buy technology that has already been certified or designated as a qualified anti-terrorism technology by DHS.

Of course, since 85% of our critical infrastructure is in private sector hands, this is also an important community that needs to appreciate the SAFTEY Act's benefit. Important steps have been taken in this regard, most recently through the release of the National Infrastructure Protection Plan, which includes a section on the SAFETY Act and outlines its benefits for critical infrastructure owners and operators.

Conclusion

In conclusion, we congratulate DHS for drafting and issuing a final rule that sets the appropriate legal framework for the deployment of anti-terrorism technologies, services and systems by federal, state, local and commercial buyers. This regulation will help make us safer by providing needed protection for vendors and buyers.

We also would note the excellent work that has been done drafting a new application kit that effectively implements this regulation.

At the same time, more needs to be done to have this program realize its true potential. As I have just outlined, issuing a new application kit with streamlined review processes; building the SAFETY Act into the acquisition process early on; training procurement and acquisition officials at all levels of federal, state and local government; modifying internal DHS acquisition rules; and concluding the FAR Council's work to provide needed guidance for federal government buyers are all essential steps.

Collectively, these steps will create a more robust homeland security environment where sellers of anti-terrorism technology innovate and deploy tools that most effectively protect the American public.

We thank you for this opportunity to testify today, and hope that this Committee will continue to exercise appropriate oversight to ensure that this program works to enhance the security of our homeland. We stand ready to assist you as you move forward in this effort.

Supplemental Information

Andrew Howell
Vice President, Homeland Security Policy Division
U.S. Chamber of Commerce
1615 H Street, NW
Washington, DC 20062
202-463-3100